PROCEDURE 1350.10

Issue Date: April 30, 2006
Effective Date: May 31, 2006

SUBJECT: **Authentication requirement for access to networks, systems, computers, databases, and applications.**

APPLICATION: This procedure applies to all Executive Branch Departments, Agencies, Boards or Commissions using State information technology resources including, but not limited to, networks, systems, computers, databases, and applications.

This procedure does not apply to general public access to public or open information presented in HTML, voice, video, TTD, or other web compatible formats over the Internet or through the public switched telephone network.

PURPOSE: This procedure requires the identification and use of approved personal authentication methods, appropriate for the identified level of security required, for access to State of Michigan information technology resources to prevent unauthorized access or maintain resource data integrity.

CONTACT AGENCY: Department of Information Technology (DIT)
Office of Enterprise Security

TELEPHONE: 517/241-4090

FAX: 517/241-2013

SUMMARY: This procedure requires that State agencies, using the risk and severity profile analysis defined in Procedure 1350.50, identify the level of risk and severity of any associated loss of data for all Agency information technology resources. DIT, in coordination with the Agency, will identify and implement the appropriate method and level of authentication needed to safeguard each identified resource from unauthorized access.

APPLICABLE FORMS: None

PROCEDURES:

A. The use of an appropriate and approved method of personal authentication is required for access to all State information technology resources.

B. All users authorized to access State information technology resources must provide authentication of authorized access at each access level identified in conformance with this procedure or as otherwise approved in writing by the DIT Office of Enterprise Security. Authentication must be provided whether the point of access is from within the State's systems or from a connection point external to the State.

C. Agency responsibilities:

1. Each Agency must identify the level(s) of personal authentication required for Agency-specific information technology resources.
    a. Agencies must use the risk and severity profile defined in Procedure 1350.50, Web Application Risk Assessment Framework for the Use of PKI Certificates, and select the profile best associated with the resource:
        i. Risk zero, Severity zero - Public and FOIA-able information;
            a. No authentication required,
            b. At this level, zero confidence in the identity of the end-user is needed.
        ii. Risk one, Severity one - Protected information, system, or application;
            a. User id & password authentication,
            b. At this level, moderate confidence is needed that the end-user identity is valid.
        iii. Risk one, Severity two - Protected information;
            a. Two-factor authentication or approved business process,
            b. A high confidence is required of the end-user's identity.
        iv. Risk two, Severity one - Protected information;
            a. Two-factor authentication,
            b. A high confidence is required of the end-user's identity.
        v. Risk two, Severity two - Protected information;
            a. Two-factor authentication and/or password client PKI,
            b. A very high confidence is required in the end-user's asserted identity.
2. Agencies must submit their profile for each information technology resource, in writing, to the DIT Office of Enterprise Security with a request that the appropriate technical method of authentication matching the risk and severity level be implemented.
    a. Technical methods of achieving authentication to match the risk and severity level may include:
        i. User ID and Passwords
        ii. Biometrics
        iii. Directories
        iv. Smart cards
        v. Single sign-on solutions
        vi. Tokens
        vii. PKI & Certificates
        viii. Voice recognition
        ix. Shared secrets
        x. Access control lists and files.
        xi. Unique business process.

D. DIT responsibilities:

1. The Office of Enterprise Security will refer the profile and request for authentication method to the appropriate technical custodian within DIT:
    a. Model Office and Field Services for desktop,
    b. Agency Services/Application Developers for application authentication,
    c. Technical Services for Directory/network authentication,
    d. Telecommunications and Network Management for remote access to network, or
    e. Technical and Data Center Services for server administration access.
2. The technical custodian, in coordination with the Office of Enterprise Security, will:
    a. Review the written risk and severity profile for compliance with DIT policies, procedures and standards;
    b. Determine the appropriate level of authentication, in coordination with the requesting Agency;
    c. Implement the identified level of authentication, in coordination with the requesting Agency; and
    d. Certify the fully functioning authentication method has been implemented.
3. Office of Enterprise Security will review and monitor authentication controls to ensure appropriate authentication methods are used.
4. Internal Auditor shall verify compliance with 1300 and 1400 Series policies and procedures are maintained.

E. State agencies desiring to implement practices and procedures differing from this procedure may do so only with the written approval of the DIT Office of Enterprise Security.

* * *